Multi-Objectives Model to Process Security Risk Assessment Based on AHP-PSO

Gamal A. Awad
Faculty of Computer Science, Muscat College, Sultanate Oman

Elrasheed I. Sultan & Noraziah Ahmad
Faculty of computer system and Software Engineering, University Malaysia Pahang, Kuantan 26300, Malaysia

Norafida Ithnan
Faculty of Computer Sciences, University Technology University, Johor, Malaysia

A. H. Beg
Faculty of computer system and Software Engineering, University Malaysia Pahang, Kuantan 26300, Malaysia

Received: January 22, 2011 Accepted: March 28, 2011 doi:10.5539/mas.v5n3p246

Abstract

Nowadays the security risk assessment play a crucial role, which is applied to the entire life cycle of information systems and communication technologies but still so many models for security risk assessment are non practical, therefore, it should be measured and improved. In this paper, a novel approach, in which Analytic Hierarchy Process (AHP) and Particles Swarm Optimization (PSO) can be combined with some changes, is presented. The method consists of; firstly, the analytic hierarchy structure of the risk assessment is constructed and the method of PSO comprehensive judgment is improved according to the actual condition of the information security. Secondly, the risk degree put forward is PSO estimation of the risk probability, the risk impact severity and risk uncontrollability. Finally, it gives examples to prove that this method Multi Objectives Programming Methodology (MOPM) can be well applied to security risk assessment and provides reasonable data for constituting the risk control strategy of the information systems security. Based on the risk assessment results, the targeted safety measures are taken, and the risk is transferred and reduced, which is controlled within an acceptable range.

Keywords: Risk assessment, Information security, PSO, Analytic hierarchy process, Multi-objectives model

1. Introduction

To access information system security, risk assessment is very important even in presence of uncertainty of the system. Recently, with the development of information security as backbone of maintaining sustainability and survivability of modern organizations and protecting information through conducting a practical Security Risk assessment (SRA), to ensure the security of the information system. If the potential threats which exist objectively attack the system vulnerabilities, threat and actual negative impact caused by threat source, then identify risk of information security based on possibility of threats and the extent of negative impact (Wang Yingmei, Wang Shengkai and Cheng Xiangyun, 2007). The method of Analysis of Hierarchy Process and Decision Making AHP/DM evidence theory to handle the uncertainty of the system, compared with other methods, the AHP method has been widely used in security risk assessment, for this method can change from the qualitative index into quantitative index. Realistic risk assessment involves many uncertainty factors, some of which are even unknown.

In the previous research, risk degree is relative to the probability and the impact severity of risk factors. Risk assessment methods involve OCTAVE, Analytic Hierarchy Process AHP and Dynamic Event Tree Analysis Method (DETAM), etc. (ISO/IEC15408, 1999)(Common Criteria for Information Technology Security Evaluation, 2005). All these methods have particular requirements, such as OCTAVE is nonlinear and iterative, it requires threat profiles and vulnerabilities catalog should be put forward or afterward of risk assessment.

Kendall (M. Kendall, 1962) proposed an approach where priorities were used as factors that are simply added together and then the average is taken as the majority choice. This method is used to apply to determine critical security risk areas and the choice of mitigations used, combined with the widely used risk qualitative assessment. The risk analysis can be measured using the theory of probability that estimate the likelihood and the consequences of the risk. In (Y. Deng, W.K. Shi, F. Du, 2004)(F. Du, W.K. Shi and Y. Deng, 2005) these models are not efficient due to the amount of computation time required for performing the complicated fuzzy number arithmetic operations and time for performing linguistic approximation.

At present, the methods of information security risk evaluation can be mainly divided into the three types: qualitative assessment method, quantitative assessment method and qualitative combined with quantitative assessment method. The common used assessment methods include matrix analysis, Decision-Tree, and probability analysis etc, and a lot of research achievements have been acquired.

In this paper, a new method of risk assessment for information security based on combine the AHP with the PSO algorithm, to analyze the probability and effect of risk, so that risk level of each risk factor can be determined and the risk control advice can be given. The comparison matrix of AHP is set after establishing of hierarchy, which comes by comparison of lower and upper elements and PSO comprehensive evaluation in risk analysis, and presents a scientific and effective method to calculate the final risk value of a selected information system. The advantages of the information system risk analysis are as follows: (1) Enabling to develop secure information management; (2) Supporting effective decision-making for information security policies; (3) Establishing practical security policies for organizations; (4) Providing valuable analysis data for future estimation. Finally, the research results show the proposed method is effective and easy to operate.

The rest of this paper is organized as follows: The necessary theoretical background AHP method and PSO are introduced the proposed new hierarchical risk assessment based on combination of the AHP with the PSO algorithm ,furthermore, the results demonstrated to develop the information security risk by using MOPM to improve the both method.

2. Security Risk Assessment

Security has been widely recognized as one of the main obstacles to the adoption. It is considered an important aspect in the debate over challenges facing. The performance evaluation requires a model that enables us to analyze the various imperative factors and criteria related to the quality and performance. The proposed model is based on FI operators and produces four measures of security risk attack dimensions: direct internal attack, communication tampering attack, code programming attack and denial of service attack with a hierarchical ring layer structure. Our experimental results showed that direct internal attack risk has a large impact on e-banking security performance. The results also confirm that the risk of direct internal attack for e-banking dynamic websites is doubled that of all other attacks (Wang Yingmei, Wang Shengkai and Cheng Xiangyun, 2007).

A risk assessment model is generated by combining AHP method with decision making (DM) method to solve these problems. Not only does the AHP/DM method combine the advantages of both, but also can solve uncertain problems more scientifically. A sample of how to use AHP/DM method in security risk assessment is given to prove our method (Lu Simei, Zhang Jianlin, 2009).

The rise in interconnectivity in the last few years has made computer systems and networks more vulnerable to threats as they are accessed by an ever increasing number of users (ISO/IEC15408, 1999)(Common Criteria for Information Technology Security Evaluation, 2005).

One of the main reasons behind unfruitful software development projects is that it is often too late to correct the problems by the time they are detected. It clearly indicates the need for early warning about the potential risks (Y. Deng, W.K. Shi, F. Du, 2004).

3. Method of Risk Evaluation of Information

These methods have their own relative strong and weak points. For example, the idea of the matrix analysis is that the probability of occurrence and influence of the risk event are evaluated first, and then, the risk degree of each risk event is evaluated by matrix analysis, which is more intuitive, but rather simple and less objective (F. Du, W.K. Shi and Y. Deng, 2005).

Aiming at risk management, the target of information security risk assessment is that the threats to internet and information system and its own vulnerability can be analyzed by means of scientific methods. In addition, the damage degree caused by risk can be evaluated, defending and improving measures to the possible threats should be proposed to defend and eliminate the information security risk, or control the risk within an acceptable extent, so that, internet and information security can be controlled to the maximum extent. The risk evaluation is a

process of computing risk value by mean of risk analysis. At present, the methods of information security risk evaluation can be mainly divided into the three types: qualitative assessment method, quantitative assessment method and qualitative combined with quantitative assessment method. Moreover, the common used assessment methods include matrix analysis (1), Decision-Making (2), and probability analysis (3).

The development of information technology and the popular use of the information network system, the security of the information system becomes particular important. To ensure the security of the information system, it is a key point to have risk assessment. If the potential threats which exist objectively attack the system vulnerabilities, there will be the risk which leads to destroy and lost of the system. The risk assessment is a process in which the risk is analyzed and explained.

Information security has become the backbone of maintaining sustainability and survivability of modern organizations and protecting information through conducting a practical Security Risk Assessment (SRA), as described in this paper, should be one of the fundamental components of conducting business. Information is regarded as an asset (Dong-Mei Zhao, Jing-Hong Wang, 2005) as such is exposed to various risks organizations often invest resources to address technical and procedural controls to mitigate these risks, while developing a more practical approach to SRA receive less attention because of the complexities involved in making choices for a tailored risk management method (Lu Simei, Zhang Jianlin, 2009).

There are so many models for security risk assessment, but most of them are non practical. An effective security risk management process enables enterprises to operate in the most cost efficient manner with a known and acceptable level of business risk (Marc J. Schniederjans a, Tim Garvin).

With the global information technology and the continuous advance of the popularity of internet, more and more organizations will shift or expand the course of its business into internet environment, so the importance of information systems security which are closely related to business organizations are widespread concerned. How to measure and evaluate the information systems security situation is worthy of an in-depth study by researchers. Risk assessment is the core and key of information system security. Through risk assessment, decision-makers can clearly understand the situation of information system security, where the risk comes from, what kind of measures can be carry out.

The planning is an optimization problem, which usually has more than one objective. This optimization problem should be solved under uncertainties considering its limitations. These inherent features of the problem make it complex and hard to solve. In order to find a solution, an algorithm should be used to enable us compare the different objectives of the main problem. A variety of these techniques exist which are called "Multi Attribute Decision Making" (MADM). Analytical hierarchical process (AHP) is one of those mentioned methods, which is used in this paper. In DM planning, the best plan over available options should be found.(Marc J. Schniederjans a, Tim Garvin).

The index, by which different plans are compared, is generated using AHP method. This index includes all the important factors of a good plan in planner's point of view. Therefore, to have a better answer, all the available options should be considered and the decision factors should be adjusted accurately.

4. Risk Assessment of the Information System

The AHP is a decision means with many rules to process variables which are difficult to be given a value (Common Criteria for Information Technology Security Evaluation, 2005). It can decompose the complicated situation into the much easier hierarchy structure in order to analyze step by step. It can express and deal with person's subjective judgment in quantity, also deal with the certain and uncertain factor, in addition to suggest whether the person's subjective judgment is right. It falls into four steps to resolve problem by AHP. Figure 1 shows simple system plan AHP to build network risk. In this figure the X_{ij} where matter risk.

The AHP and PSO will solve the information security risk system thought four stages; first step is constructing the hierarchy structure. The second step is constructing the judge matrix by using factor comparison. The third step is calculating the relative weight of the factors by the judge matrix. In the last step, the whole weight of the factors at each layer is calculated. In this paper, the model is applied to make decision for all steps, by which risk degree is put forward and the fuzzy logical method is used (Dong-Mei Zhao, Jing-Hong Wang, 2005). Figure 2 shows the four stages that process in this matter. The a_{ij} is factor comparison security, x_{ij} is variably stages.

5. Multi Objectives model and decision making to enhance AHP

The AHP and a Multi-Objective Programming Methodology (MOPM) as aids in making high risk system and lows cost, the application of these methodologies in ABC cost driver selection is presented. The informational efficacy of the proposed combined methodologies is also discussed (Dong-Mei Zhao, Jing-Hong Wang, 2005)

(Omkarprasad S Vaidya, 2006). In this paper the MOPM contain two objectives, first objective for the maximum security system and second one minimum the cost plan. Formula 1 and 2 are present the both objectives. Moreover, formula 3, 4, and 5 are the subjective for the model. The applications MOPM of AHP is to assist the decision-making tool that has been used in all applications related with decision-making. The formula 1 and 2 are objectives and 3, 4 and 5 are the subjective model

$$Max\ Z_1 = \sum_{n=1}^{k} \quad \sum_{i=1}^{n} \quad \sum_{j=1}^{m} R \quad {}_n X_{ij} \qquad ------(1)$$

$$Min_{1\le R\le k}\ Z_2 = \sum_{i=1}^{n} \quad \sum_{j=1}^{m} C_{ij} \qquad ------------(2)$$

$$Subjectives$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} \quad a_{ij}\, X_{ij} \le b_{ij} \qquad ----------(3)$$

$$\sum_{l=1}^{k} R_l \le t_l \qquad ----------(4)$$

$$0 \le X_{ij} \le s_i \qquad ----------(5)$$

$$X_{ij} > 0\ , R_i > 0\ , C_{ij} > 0$$

$$0 < a_{ij} \le 1$$

Where:

k= number of lump

n= number of section

m=number of unit

R=name of lump

X_{ij} *= variable percentage of risk effective*

C_{ij}*= cost percentage*

a_{ij} *= the strength of each part i*

b_{ij}*= total capacity for all* X_{ij}

t_l*= total capacity for all* R_l

s_i*= cost percentage of each* X_{ij}

6. Conclusion

The Information security risk assessment is an important matter today as the services and customers continue looking for batter system plan. The AHP and PSO can be combined to get superior solution by using MOPM. The method consists of; firstly, the analytic hierarchy structure of the risk assessment is constructed and the method of PSO comprehensive judgment is improved according to the actual condition of the information security. The MOPM model can get the maximum security that is depend on percent risk which limited for mange, also the model will select the lower cost method which give security depend on the risk.

References

Common Criteria for Information Technology Security Evaluation. (2005). v3.0, June 2005.

Dong-Mei Zhao, Jing-Hong Wang. (2005). Using Fuzzy Logic And Entropy Theory To Risk Assessment Of The Information Security, Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 2005.

F. Du, W.K. Shi and Y. Deng. (2005). New similarity measure of generalized fuzzy numbers, *Journal of Shanghai Jiaotong University,* vol.39, no. 8, pp. 614-617, 2005.

ISO/IEC15408. (1999). Common Criteria for IT Security Evaluation. Version 2.1. The International Organization for Standardization, 1999.

Lu Simei, Zhang Jianlin. (2009). Security Risk Assessment Model Based on AHP/D-S Evidence Theory, International Forum on Information Technology and Applications, 2009.

M. Kendall. (1962). *Rank correlation methods.* 3rd ed.; 1962. NY.

Marc J. Schniederjans a, Tim Garvin. Using the Analytic Hierarchy Process and multi-objective programming for the selection of cost drivers in activity-based costing.

Omkarprasad S Vaidya, Sushil Kumar. (2006). Analytic hierarchy process: An overview of applications, *European Journal of Operational Research* 169 (2006) 1–29.

Wang Yingmei, Wang Shengkai and Cheng Xiangyun. (2007). *Security Risk Assessment of Information System,* Publishing House of Electronic Industry, Beijing, 2007.

Y. Deng, W.K. Shi, F. Du. (2004). A new similarity measure of generalized fuzzy numbers and its application to pattern recognition, *Pattern Recognition Letters,* vol.24, no. 8, pp. 875-883, 2004.

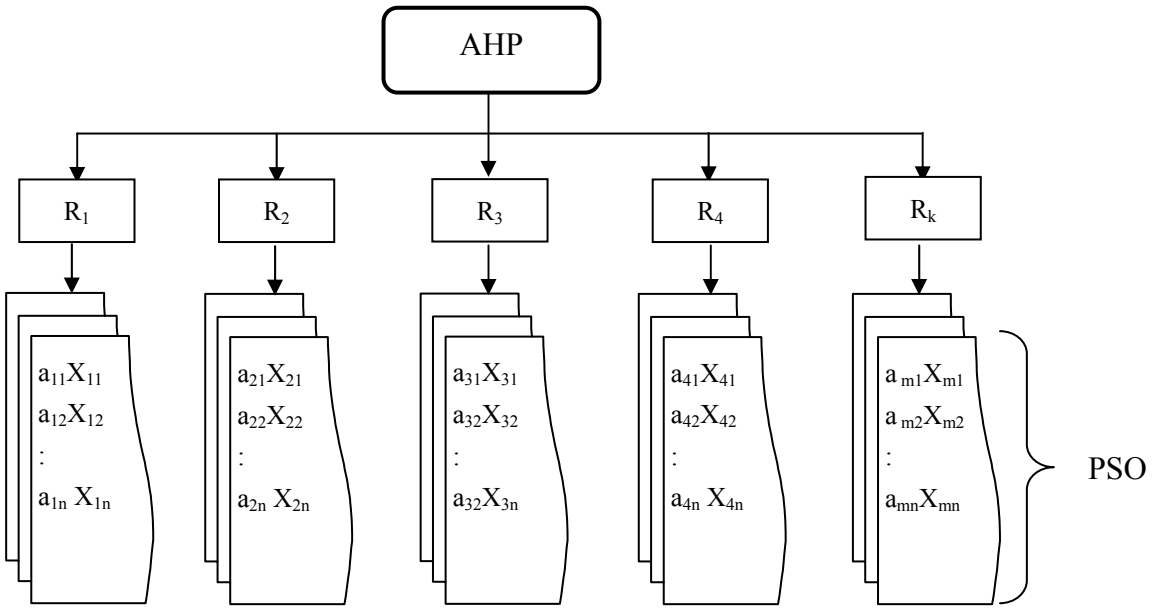

Figure 1. System plan of AHP

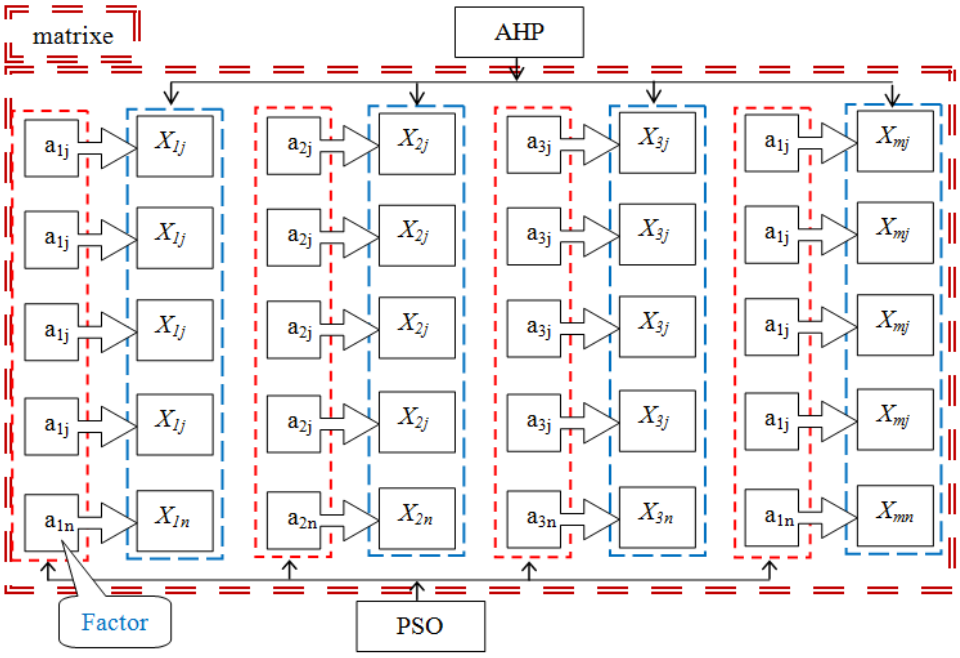

Figure 2. Maternal AHP & PSO